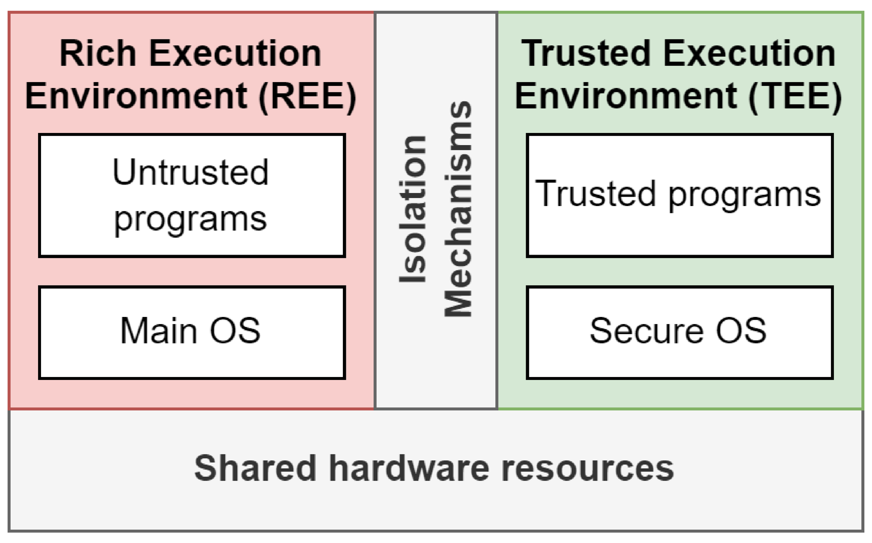
Internal Power-Management-based Fault Attacks

Gwenn Le Gonidec [1], Maria Méndez Real [2], Guillaume Bouffard [3], Jean-Christophe Prévotet [4]

[1]IETR, INSA Rennes, France
[2]Lab-STICC, Université Bretagne Sud, Lorient, France
[3]Agence nationale de la Sécurité des Systèmes d'Information (ANSSI), France
[4]IETR, INSA Rennes, France
Contact : owen.le-gonidec@insa-rennes.fr

Project ANR JCJC **CoPhyTEE**,
contract ANR-23-CE39-0003-01

Trusted Execution Environments (TEEs) at risk



→ Used in a large variety of devices and applications

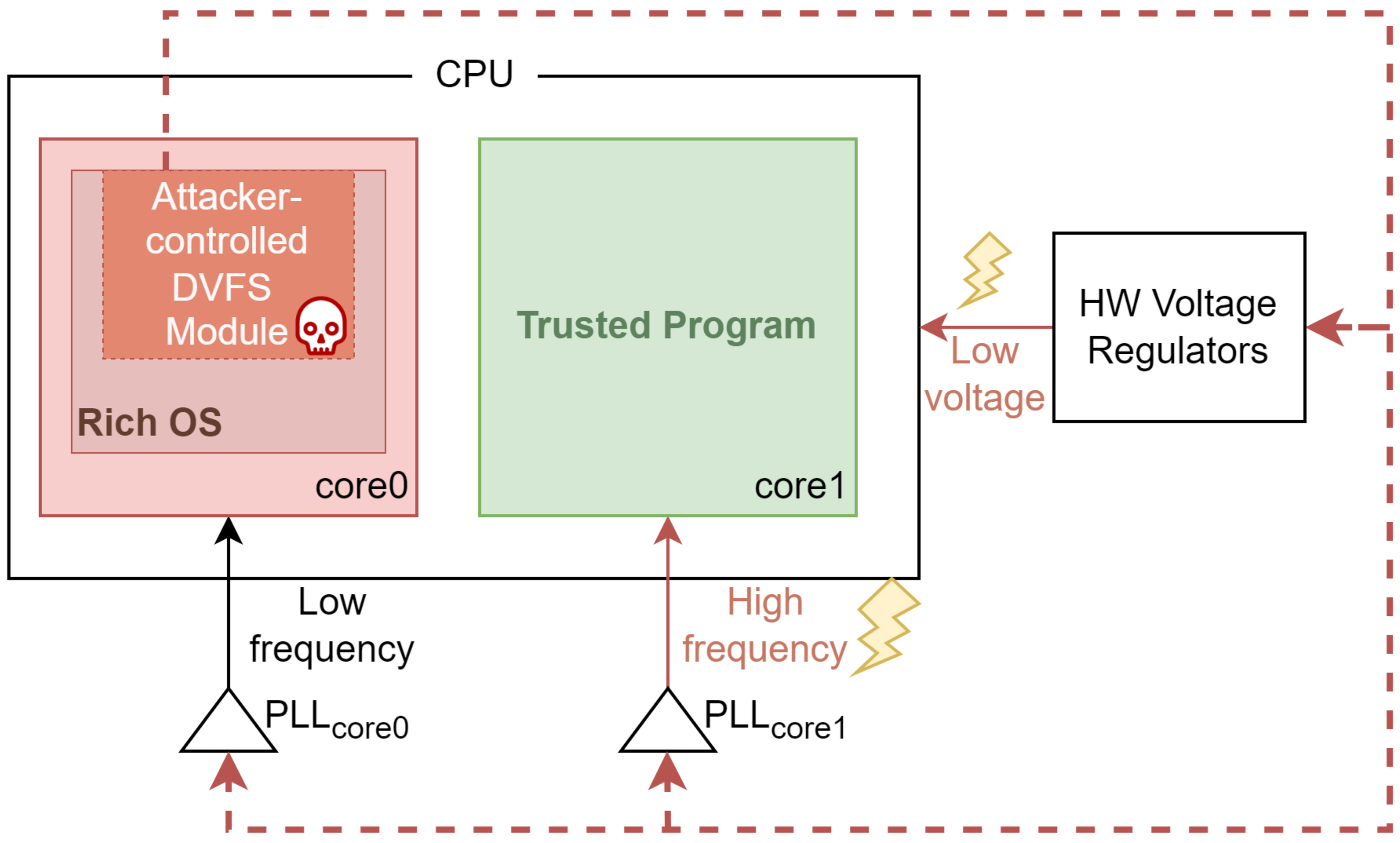
- Remote telemetry (MCUs, IoT)
- Digital Rights Managements, biometry (CPUs)
- Confidential computing (cloud servers)

Complex systems → **wide attack surface**

Vulnerability: Attacks through **shared hardware**

Power-Management-based Attacks

Power management modules make **voltage** & **frequency** regulators controllable by software ⇒ software-induced **Clock Glitch**



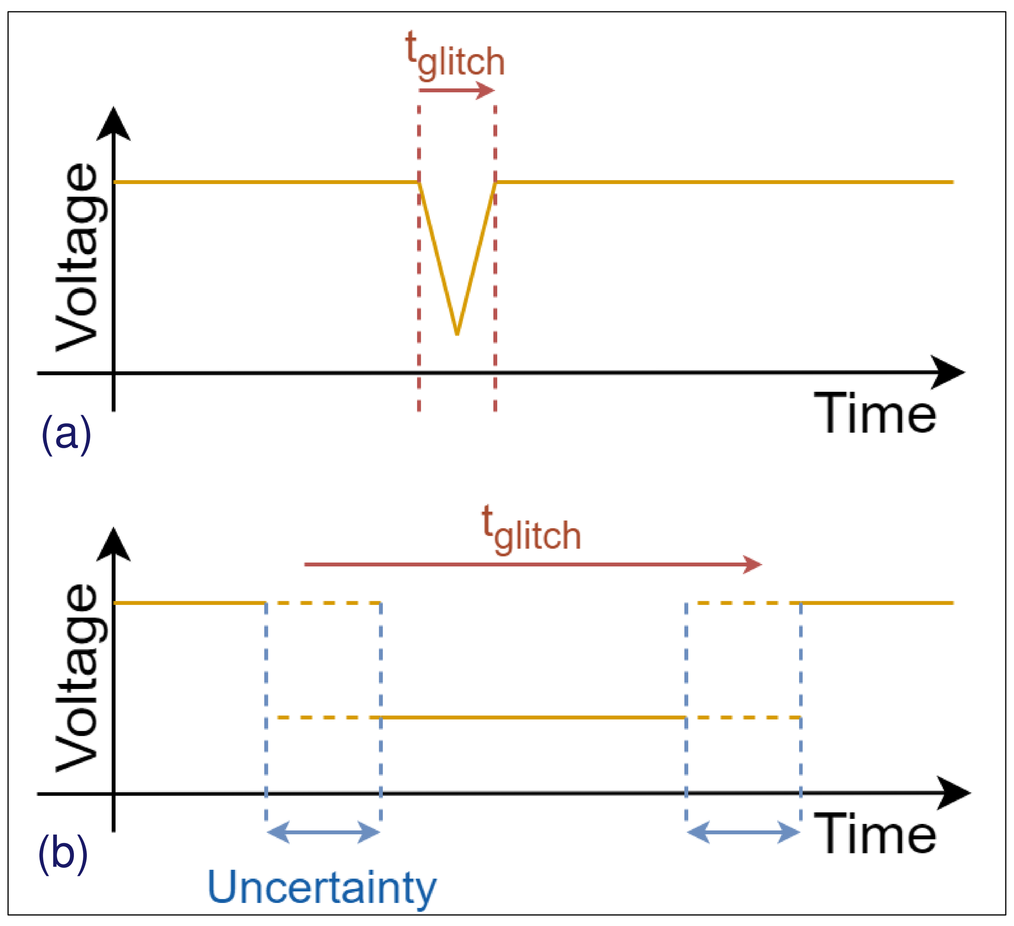
Software-Induced Attack	This Attack	Hardware Attack
Remote attacker model → **Massive** and simultaneous exploitation		• Powerful fault models • Well-known characterization and exploitation methods

Exploitation scenarios demonstrated in the literature:

- **Extract cipher keys** from the TEE using Differential Fault Analysis
- Force an **out-of-bounds** memory access to occur
- Fault verification steps to launch an **ill-signed program** in the TEE
- Denial-of-Service

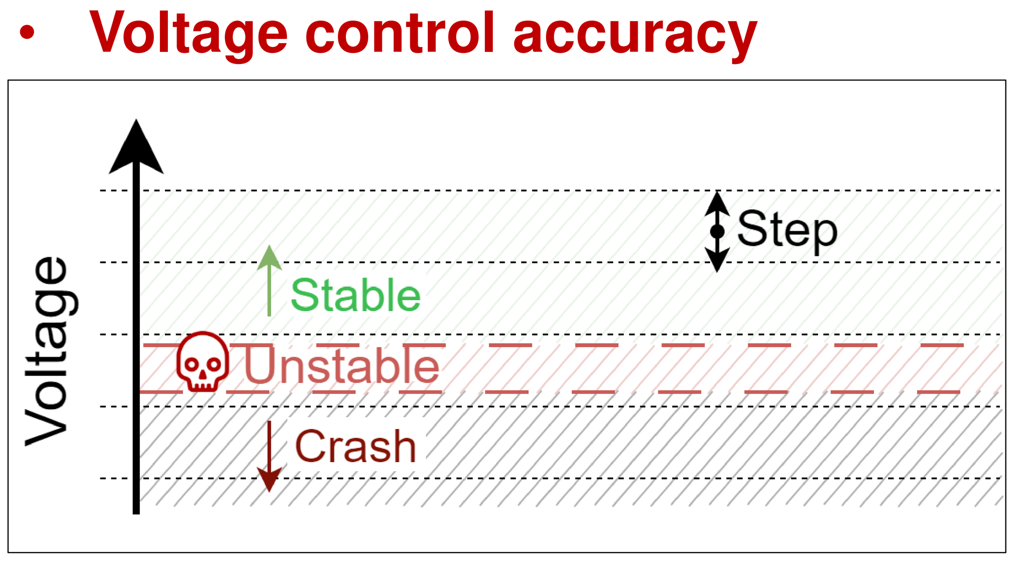
Limitations

- **Timing accuracy**



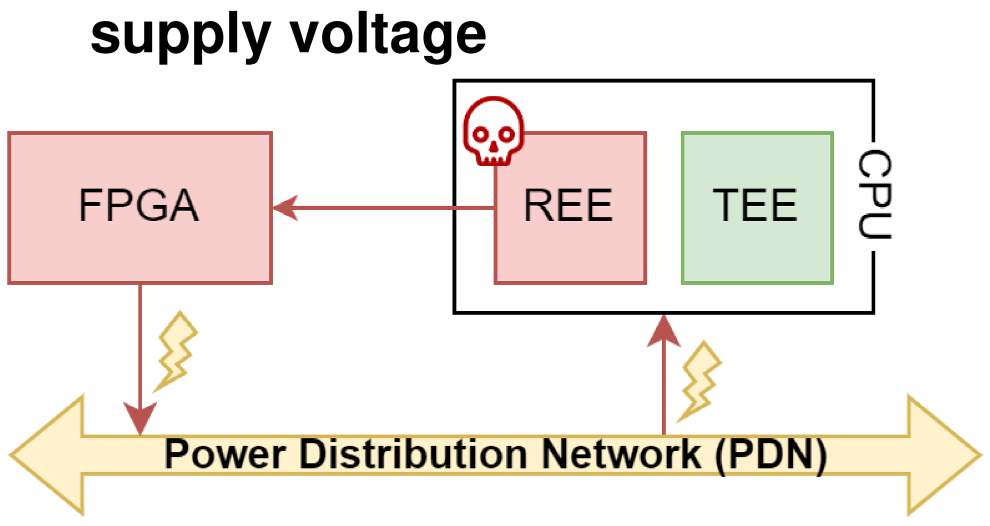
(a) Ideal scenario, (b) Actual precision

- **Voltage control accuracy**

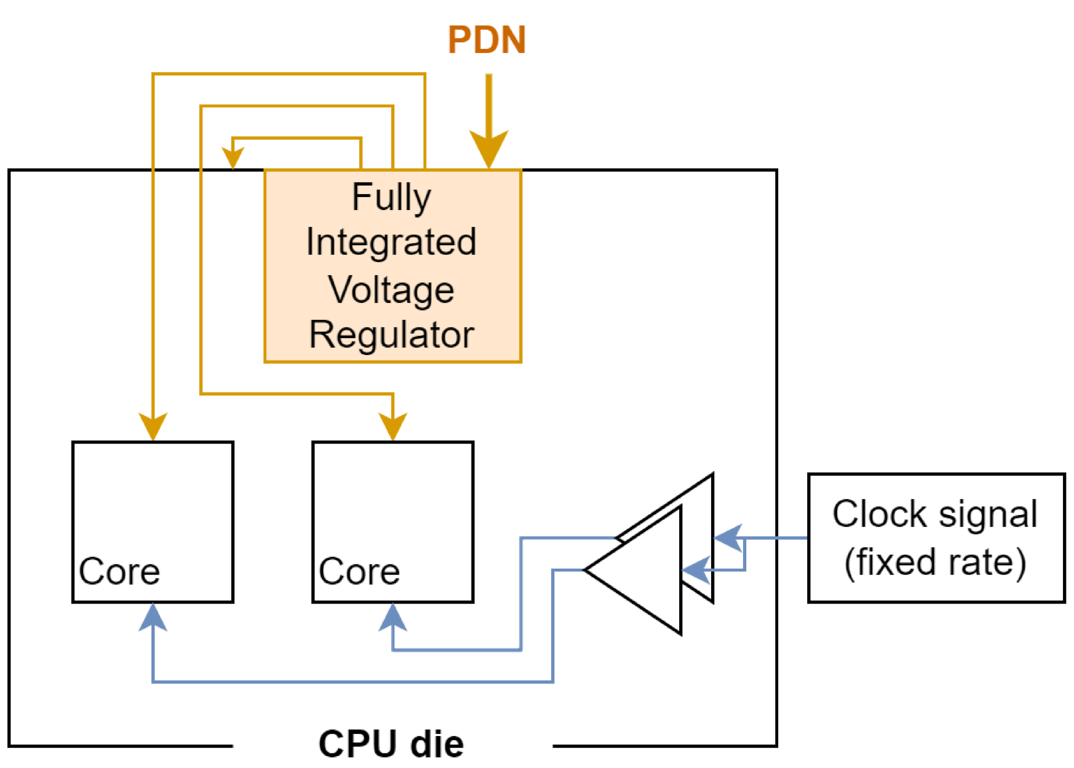


Improvements

- **Combination with other attacks**
- **New ways to manipulate the supply voltage**

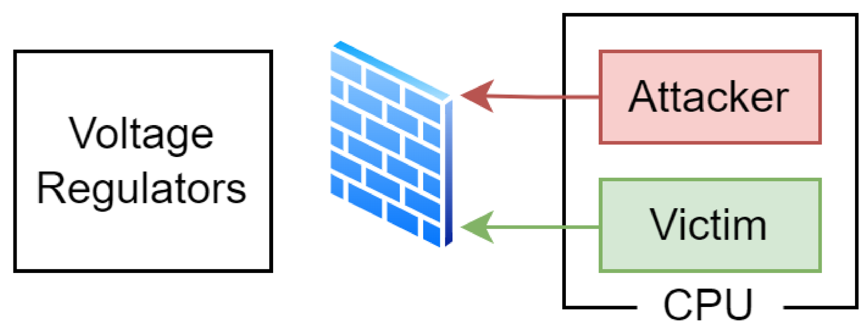


- **Evolution of power management mechanisms**



Countermeasures

- **Arm and Intel's response: deactivate software access to voltage management interfaces**



→ Impact on energy management mechanisms?
→ What about indirect ways to manipulate voltage?

- **Many approaches explored in the litterature**
  - Software-level countermeasures for trusted applications
  - Strengthen the CPU's pipelines against undervolting
  - Co-processor for voltage regulators access control

→ Cost / overhead / efficiency balance

Additional details are given in the article — from the same authors, ***Do Not Trust Power Management: A Survey on Internal Energy-based Attacks Circumventing Trusted Execution Environments Security Properties***, 2024, available at: https://doi.org/10.48550/arXiv.2405.15537

Main references: Tang *et al.*, *CLKSCREW*, 2017 — Murdock *et al.*, *Plundervolt*, 2020 — Mahmoud *et al.*, *DFaulted*, 2022